UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

APRIL COOK, on behalf of her minor child S.C., and on behalf of all others similarly situated, Plaintiff, v. CDHA MANAGEMENT, LLC d/b/a CHORD SPECIALTY DENTAL PARTNERS and SPARK DSO, LLC d/b/a CHORD SPECIALTY DENTAL PARTNERS, Defendants.	Case No. _____ Class Action Jury Demand

CLASS ACTION COMPLAINT

Plaintiff April Cook, on behalf of her minor child S.C. ("Plaintiff"), on behalf of herself and all others similarly situated, alleges the following (the "Action") against CDHA Management, LLC d/b/a Chord Specialty Dental Partners and Spark DSO, LLC d/b/a Chord Specialty Dental Partners ("Chord") upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

I. INTRODUCTION

1. Plaintiff seeks monetary damages and injunctive and declaratory relief arising from Chord's failure to safeguard the Personally Identifiable Information[1] ("PII") and Protected Health

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Chord, not every type of information included in that definition was compromised in the subject data breach.

Information ("PHI") (together, Private Information") of its patients, which resulted in unauthorized access to its information systems between August 19, 2024 and September 25, 2024, and the compromised and unauthorized disclosure of that Private Information, causing widespread injury and damages to Plaintiff and the proposed (defined below) members.

2. Chord is a dental support organization headquartered in Tennessee that provides support services to over 60 dental practices in six states.[2]

3. As explained in detail herein, Chord detected unusual activity related to an employee email account and ultimately determined that an unauthorized third party accessed a few employees' email accounts and obtained certain files between August 19, 2024, and September 25, 2024 ("Data Breach").[3]

4. As a result of the Data Breach, which Chord failed to prevent, the Private Information of Chord's patients including Plaintiff and the proposed Class members, were stolen, including their names, addresses, Social Security numbers, driver's licenses, bank account information, payment card information, dates of birth, medical information, and health insurance information.[4]

5. Chord's investigation concluded that the Private Information compromised in the Data Breach included Plaintiff's and other Class Members information (together, "patients").

6. Chord's failure to safeguard patients' highly sensitive Private Information as exposed and unauthorizedly disclosed in the Data Breach violates its common law duty, Tennessee law, and Chord's implied contract with patients to safeguard their Private Information.

---

[2] https://www.chordsdp.com/ (last visited Apr. 1, 2025).
[3] *See* https://www.chordsdp.com/notification-of-data-security-incident/; Notice of Data Breach ("Notice Letter"), attached hereto as ***Exhibit A*.**
[4] https://www.chordsdp.com/notification-of-data-security-incident/ (last visited Apr. 1, 2025).

7. Plaintiff and Class members now face a lifetime risk of identity theft due to the nature of the information lost, which they cannot change, and which cannot be made private again.

8. Chord's harmful conduct has injured Plaintiff and Class members in multiple ways, including: (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

9. Chord's failure to protect Plaintiff's and Class members' Private Information has harmed and will continue to harm thousands of patients, causing Plaintiff to seek relief on a class wide basis.

10. On behalf of herself and the Class preliminarily defined below, Plaintiff brings causes of action against Chord for negligence, negligence *per se*, breach of fiduciary duty, and breach of implied contract, seeking an award of monetary damages and injunctive and declaratory relief, resulting from Chord's failure to adequately protect their highly sensitive Private Information.

II. JURISDICTION AND VENUE

11. The Court has subject-matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100 and at least one Class member is a citizen of a state that is diverse from Chord's citizenship, namely Plaintiff, a citizen of Pennsylvania. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

12. This Court has personal jurisdiction over Chord because it has its headquarters and principal place of business in Tennessee and does a significant amount of business in Tennessee.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Chord has its headquarters and principal place of business in this District, and a substantial part of the events giving rise to this action occurred in this District.

III. PARTIES

14. Plaintiff April Cook, on behalf of her minor child S.C.. are citizens of Tennessee and was sent a Notice from Chord dated March 14, 2025.

15. CDHA Management, LLC is a Delaware corporation with its headquarters and principal place of business located in West Chester, PA.

16. Spark DSO, LLC is a Pennsylvania limited liability company with its headquarters and principal place of business located at 1801 West End Ave, Suite 410, Nashville, Tennessee 37203.

IV. FACTUAL ALLEGATIONS

Chord's Business

17. According to Chord's website:

> "Chord Specialty Dental Partners is a Dental Support Organization dedicated to expanding access to quality dental care for children and adults, supporting over 60 practices across six states. Our goal is to ensure our partners have the right resources and processes to better serve their patients. We're committed to providing the highest level of business and operational support, allowing the dental care teams to focus on patient-centered care."[5]

18. Plaintiff and Class members are current or former patients who provided their Private Information, directly or indirectly, to Chord.

[5] https://www.chordsdp.com/about/ (last visited Apr. 1, 2025).

19. Prior to receiving services from Chord, Plaintiff and Class Members were required to and did, in fact, turn over their Private Information.

20. The information held by Chord at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class members.

21. Upon information and belief, Chord made promises and representations to its patients that the Private Information collected would be kept safe and confidential, the privacy of that information would be maintained, and Chord would delete any sensitive information after it was no longer required to maintain it.

22. Plaintiff and Class members provided their Private Information to Chord with the reasonable expectation and mutual understanding that Chord would comply with its obligations to keep such information confidential and secure from unauthorized access.

23. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class members relied on the sophistication of Chord to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

24. Chord had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class members from involuntary disclosure to third parties. Chord has a legal duty to keep patients' Private Information safe and confidential.

25. Chord had obligations under the FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

26. Chord derived a substantial economic benefit from collecting Plaintiff's and Class members' Private Information. Without the required submission of Private Information, Chord could not perform the services it provides.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Chord assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' Private Information from disclosure.

The Attack and Data Breach

28. On or about March 14, 2025, Chord began notifying affected patients of the Data Breach, informing them by Notice of Data Breach ("Notice")[6]:

> On or around September 11, 2024, CDHA Management, LLC and Spark DSO, LLC dba Chord Specialty Dental Partners ("Chord") discovered suspicious activity related to an employee's email account. Upon discovery, we took immediate action to secure the account and engaged a team of third-party specialists to assist with determining the full nature and scope of the incident. The investigation determined that an unauthorized individual had gained access to several accounts for a limited time between August 19, 2024, to September 25, 2024. Therefore, we conducted a comprehensive review of the information potentially affected. The type of information varies by individual and may include name and one or more of the following: address, Social Security number, driver's license, bank account information, payment card information, date of birth, medical information, and health insurance information.[7]

29. Chord did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

[6] https://www.chordsdp.com/notification-of-data-security-incident/ (last visited Apr. 1, 2025).
[7] *Id.*

30. The attacker accessed and acquired files in Chord's computer systems containing unencrypted Private Information of Plaintiff and Class members, including their names, addressees, Social Security numbers, driver's licenses, bank account information, payment card information, dates of birth, medical information, and health insurance information. Plaintiff's and Class members' Private Information was accessed and stolen in the Data Breach.

31. Plaintiff further believes his Private Information, and that of Class members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Chord Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information

32. As a condition to obtain services from Chord and its partners, Plaintiff and Class members were required to give their sensitive and confidential Private Information to Chord.

33. Chord retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class members' Private Information, Chord would be unable to perform its services.

34. By obtaining, collecting, and storing the Private Information of Plaintiff and Class members, Chord assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

35. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Chord to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

36. Chord could have prevented this Data Breach by properly securing and encrypting the emails and email servers containing the Private Information of Plaintiff and Class members.

37. Upon information and belief, Chord made promises to Plaintiff and Class members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

38. Chord's negligence in safeguarding the Private Information of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Chord Knew or Should Have Known of the Risk of a Cyber Attack Because Healthcare Entities in Possession of Private Information Are Particularly Suspectable to Cyber Attacks

39. Data thieves regularly target entities in the healthcare industry like Chord due to the highly sensitive information that they maintain. Chord knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

40. Chord's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities like Chord that collect and store Private Information and other sensitive information, preceding the date of the Data Breach.

41. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Chord knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

42. For example, of the 1,862 recorded data breaches in 2021, 330 of them, or 17.7%, were in the medical or healthcare industry.[8]

43. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[9]

44. Entities in custody of PHI and/or medical information reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[10] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[11] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. 40 percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[12]

45. Despite the prevalence of public announcements of data breach and data security compromises, Chord failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from being compromised.

---

[8] 2021 Data Breach Annual Report (ITRC, Jan. 2022), https://notified.idtheftcenter.org/s/, at 6.
[9] *Id*.
[10] *See* Identity Theft Resource Center, *2022 Annual Data Breach Report*, https://www.idtheftcenter.org/publication/2022-data-breach-report/ (last accessed May 8, 2024).
[11] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed May 8, 2024).
[12] *See id.*

46. Chord was, or should have been, fully aware of the unique type and the significant volume of data on Chord's server(s), amounting to thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

47. The injuries to Plaintiff and Class members were directly and proximately caused by Chord's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

48. The ramifications of Chord's failure to keep secure the Private Information of Plaintiff and Class members are long-lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

49. As a healthcare entity in possession of its patients' Private Information, Chord knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members because of a breach. Nevertheless, Chord failed to take adequate cybersecurity measures to prevent the Data Breach.

Chord Failed to Comply with FTC Guidelines

50. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

51. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

understand their network's vulnerabilities; and implement policies to correct any security problems.[13]

52. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[14]

53. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. These FTC enforcement actions include actions against healthcare entities, like Chord. *See, e.g.*, *In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data

[13] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 8, 2024).
[14] *Id.*

security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

56. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Chord, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Chord's duty in this regard.

57. Chord failed to properly implement basic data security practices.

58. Chord's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act,15 U.S.C. § 45.

Chord Failed to Comply with HIPAA Guidelines

59. Chord is covered businesses under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

60. Chord is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[15] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

[15] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

61. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

62. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

63. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

64. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

65. HIPAA's Security Rule requires Chord to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

66. HIPAA also requires Chord to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Chord is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons

or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

67. HIPAA and HITECH also obligates Chord to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

68. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

69. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

70. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance

Material.[16] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[17]

Chord Owed Plaintiff and Class Members a Duty to Safeguard their Private Information

71. In addition to its obligations under federal and state laws, Chord owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Chord owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class members.

72. Chord owed a duty to Plaintiff and Class members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

73. Chord owed a duty to Plaintiff and Class members to implement processes that would detect a compromise of Private Information in a timely manner.

74. Chord owed a duty to Plaintiff and Class members to act upon data security warnings and alerts in a timely fashion.

---

16 https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed Feb. 13, 2024)

[17]https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed Feb 13, 2024).

75. Chord owed a duty to Plaintiff and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

76. Chord owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices.

The Data Breach Increases Plaintiff's and Class members' Risk of Identity Theft

77. The unencrypted Private Information of Plaintiff and Class members will end up (if it has not already ended up) for sale on the dark web, as that is the *modus operandi* of hackers.

78. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members.

79. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class members because of the Data Breach.

80. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

81. Plaintiff's and Class members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class members and to profit from their misfortune.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

82. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

83. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class members must monitor their financial accounts for many years to mitigate the risk of identity theft.

84. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

85. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[18]

86. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports,

[18] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed May 8, 2024).

contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[19]

87. And for those Class members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

Diminution of Value of Private Information

88. Private Information is valuable property.[20] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

89. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach is difficult, if not impossible, to change.

90. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm Reseal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black

[19] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed May 8, 2024).
[20] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed May 8, 2024) ("GAO Report").

market."[21]

91. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[22]

92. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[23] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[24,25] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[26]

93. As a result of the Data Breach, Plaintiff's and Class members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed May 8, 2024).
[22] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[23] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed May 8, 2024).
[24] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed May 8, 2024).
[25] https://datacoup.com/ (last accessed May 8, 2024).
[26]https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed May 8, 2024).

data has been lost, thereby causing additional loss of value.

94. The fraudulent activity resulting from the Data Breach may not come to light for years.

95. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

96. Chord was, or should have been, fully aware of the unique type and the significant volume of data on Chord's network, amounting to millions of individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

97. The injuries to Plaintiff and Class members were directly and proximately caused by Chord's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

98. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

99. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

100. Consequently, Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

101. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor and protect Class members from the risk of identity theft resulting from Chord's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class members would not need to bear, but for Chord's failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

102. Furthermore, Chord's poor data security deprived Plaintiff and Class members of the benefit of their bargain. When agreeing to pay Chord or its partners for the provision of its services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Chord did not provide the expected data security. Accordingly, Plaintiff and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Chord.

Plaintiff's Experience

103. S.C. obtained dental care or related services from one of Chord's clients. To obtain Chord's services, S.C. was required to provide their Private Information, indirectly, to Chord.

104. Upon information and belief, at the time of the Data Breach, Chord retained S.C.'s Private Information in its system.

105. According to the Notice, S.C.'s Private Information was improperly accessed and obtained by unauthorized third parties. The Private Information comprised their name, date of birth, and medical information.

106. As a result of the Data Breach, S.C. is presently at risk and will continue to be at increased risk of identity theft and fraud for his lifetime.

107. As a result of the Data Breach, S.C. made reasonable efforts to mitigate the impact of the Data Breach, and fears for their personal financial security and uncertainty over what medical information was revealed in the Data Breach. This is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

108. S.C. has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Chord's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

109. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3), on behalf of a class defined as:

> All individuals whose PII and/or PHI was accessed and/or acquired by an unauthorized party in the Data Breach, including all who were sent a notice of the Data Breach.

110. Excluded from the Class are the following individuals and/or entities: Chord and Chord's parents, subsidiaries, affiliates, officers and directors, and any entity in which Chord has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

111. Plaintiff reserves the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

112. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief thousands of individuals had their PII compromised in this Data Breach. The identities of Class Members are ascertainable through Chord's records, Class Members' records, publication notice, self-identification, and other means.

113. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Chord had a duty to protect the Private Information of Plaintiff and Class members;

b. Whether Chord had respective duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

c. Whether Chord had respective duties not to use the Private Information of Plaintiff and Class members for non-business purposes;

d. Whether Chord failed to adequately safeguard the Private Information of Plaintiff and Class members;

e. Whether Chord failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Chord adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Plaintiff and Class members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Chord's wrongful conduct; and

h. Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

114. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

115. This class action is also appropriate for certification because Chord acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Chord's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Chord's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

116. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

117. **Predominance.** Chord has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Chord's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

118. **Superiority.** A class action is superior to other available methods for the fair and

efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Chord. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

119. Chord has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

120. Further, Chord has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

a. Whether Chord owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Chord's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Chord's failure to institute adequate protective security measures amounted to negligence;

d. Whether Chord's failure to institute adequate protective security measures amounted to breach of an implied contract;

e. Whether Chord failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to HIPAA and FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

121. Finally, all members of the proposed Class are readily ascertainable. Chord has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Chord.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and all Class Members)

122. Plaintiff repeats and realleges the above allegations as if fully stated herein.

123. Chord requires its patients, including Plaintiff and Class members, to submit non-public Private Information in the ordinary course of providing its services.

124. Chord gathered and stored the Private Information of Plaintiff and Class members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

125. Plaintiff and Class members entrusted Chord with their Private Information with the understanding that Chord would safeguard their information.

126. Chord had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

127. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Chord had a duty of care to use reasonable means to secure and safeguard their computer property—and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Chord's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

128. Chord's duty to use reasonable security measures under HIPAA required Chord to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

129. Chord owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its emails, systems, and networks, and the personnel responsible for them, adequately protected the Private Information.

130. Chord's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Chord and patients. That special relationship arose because Plaintiff and Class members entrusted Chord with their confidential Private Information, a necessary part of being patients of Chord.

131. Chord's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Chord is bound by industry standards to protect confidential Private Information.

132. Chord was subject to an "independent duty," untethered to any contract between Chord and Plaintiff or the Class.

133. Chord breached its duties, thus were negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Chord include, but are not limited to, (a) failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information; (b) failing to adequately monitor the security of their networks and systems; and (c) allowing unauthorized access to Class members' Private Information.

134. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly considering Chord's inadequate security practices.

135. It was foreseeable that Chord's failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

136. Chord had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

137. Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Chord knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and Class members, the critical

importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Chord's systems.

138. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

139. Plaintiff and Class members had no ability to protect their Private Information that was in, and likely remains in, Chord's possession.

140. Chord was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

141. Chord's duty extended to protecting Plaintiff and Class members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

142. Chord has admitted that the Private Information of Plaintiff and Class members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

143. But for Chord's wrongful and negligent breach of duties owed to Plaintiff and Class members, the Private Information of Plaintiff and Class members would not have been compromised.

144. There is a close causal connection between Chord's failure to implement security measures to protect the Private Information of Plaintiff and Class members and the harm, or risk of imminent harm, suffered by Plaintiff and Class members. The Private Information of Plaintiff and Class members was lost and accessed as the proximate result of Chord's failure to exercise

reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

145. As a direct and proximate result of Chord's negligence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Chord's possession and is subject to further unauthorized disclosures so long as Chord fails to undertake appropriate and adequate measures to protect the Private Information.

146. As a direct and proximate result of Chord's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

147. Additionally, as a direct and proximate result of Chord's negligence, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Chord's possession and is subject to further unauthorized disclosures so long as Chord fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

148. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

149. Plaintiff and Class members are also entitled to injunctive relief requiring Chord to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and all Class Members)

150. Plaintiff repeats and realleges the above allegations as if fully stated herein.

151. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Chord had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

152. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., Chord had a duty to implement reasonable safeguards to protect Plaintiff's and Class members' Private Information.

153. Pursuant to HIPAA, Chord had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

154. Chord breached its duties to Plaintiff and Class members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

155. Chord's failure to comply with applicable laws and regulations constitutes negligence *per se.*

156. The injuries to Plaintiff and Class members resulting from the Data Breach were directly and indirectly caused by Chord's violation of the statutes described herein.

157. Plaintiff and Class members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

158. But for Chord's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

159. The injuries and harms suffered by Plaintiff and Class members were the reasonably foreseeable result of Chord's breach of its duties. Chord knew or should have known that it was failing to meet its duties and that Chord's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

160. As a direct and proximate result of Chord's negligent conduct, Plaintiff and Class members have suffered injuries and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiff and all Class Members)

161. Plaintiff repeats and realleges the above allegations as if fully stated herein.

162. On information and belief, Chord entered into contracts to provide services to its clients, which services included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be provided to it.

163. On information and belief, these contracts are virtually identical and were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Chord agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

164. Chord knew that if it were to breach these contracts with its clients, the clients' patients, including Plaintiffs and the Class Members, would be harmed.

165. Chord breached its contracts with its clients—whose members, including Plaintiffs and the Class Members—were affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach, and when it failed to timely notify Plaintiffs and Class Members regarding the Data Breach.

166. As foreseen, Plaintiffs and the Class Members were harmed by Chord's failure to use reasonable data security measures to store the Private Information Plaintiffs and Class Members provided to their respective health plans or other entities who in turn provided that information to Chord and the failure to timely notify Plaintiffs and Class Members, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

167. Accordingly, Plaintiffs and the Class Members suffered and will suffer injury including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Personal Information which

remains in Chord's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Personal Information compromised as a result of the Data breach; (vii) loss of potential value of their Personal Information; (viii) overpayment for the services that were received without adequate data security.

168. Accordingly, Plaintiffs and the Class Members are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class members, requests judgment against Chord and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Chord from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting Chord from engaging in the wrongful and unlawful acts described herein;

ii. requiring Chord to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Chord to delete, destroy, and purge the Private Information of Plaintiff and Class members unless Chord can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iv. requiring Chord to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class members;

v. prohibiting Chord from maintaining the Private Information of Plaintiff and Class members on a cloud-based database;

vi. requiring Chord to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Chord's systems on a periodic basis, and ordering Chord to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Chord to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Chord to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Chord to segment data by, among other things, creating firewalls and access controls so that if one area of Chord's network is compromised, hackers cannot gain access to other portions of Chord's systems;

x. requiring Chord to conduct regular database scanning and security checks;

xiv. requiring Chord to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Chord's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Chord to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. requiring Chord to implement logging and monitoring programs sufficient to track traffic to and from Chord's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis to evaluate Chord's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined by a jury at trial;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury.

DATED: April 3, 2025

Respectfully submitted,

/s/ Gerard J. Stranch IV
Gerard J. Stranch IV, PBR 23045
Grayson Wells, BPR 39658
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Counsel for Plaintiff and the Class